Legislative Language

Law Enforcement Provisions Related to Computer Security

Part 1: Specific Criminalization of Damaging Critical Infrastructure Computers

Title 18, United States Code, is hereby amended to add the following section –

§ 1030A. Aggravated Damage to a Critical Infrastructure Computer

(a) Offense.—

(1) Whoever, during and in relation to a felony violation of section 1030 of this title knowingly causes or attempts to cause damage to a critical infrastructure computer, and such damage results in (or, in the case of an attempted offense, would, if completed have resulted in) the substantial impairment—

(A) of the operation of the critical infrastructure computer; or

(B) of the critical infrastructure associated with such computer,

shall, in addition to the term of punishment provided for such felony, be sentenced to a term of imprisonment of 3 years.

(b) Consecutive sentence.—Notwithstanding any other provision of law—

(1) a court shall not place on probation any person convicted of a violation of this section;

(2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment, including any term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony violation of Title 18, United States Code, Section 1030;

(3) in determining any term of imprisonment to be imposed for the felony violation of Title 18, United States Code, Section 1030, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section; and

(4) a term of imprisonment imposed on a person for a violation of this section may, in the discretion of the court, run concurrently, in whole or in part, only with another term of imprisonment that is imposed by the court at the same time on that person for an additional violation of this section, provided that such discretion shall be exercised

in accordance with any applicable guidelines and policy statements issued by the Sentencing Commission pursuant to section 994 of title 28.

(c) Definitions.—In this section—

(1) the terms "damage" and "computer" have the meanings set forth for such terms in section 1030 of this title; and

(2) the term "critical infrastructure computer" means a computer that manages or controls systems or assets vital to national defense, national security, national economic security, public health or safety, or any combination of those matters, whether publicly or privately owned or operated, including gas and oil production, storage, and delivery systems; water supply systems; telecommunication networks; electrical power delivery systems; finance and banking systems; emergency services; transportation systems and services; and government operations that provide essential services to the public.

Part 2: Clarifying the Scope and Penalties for Offenses under the Computer Fraud and Abuse Act

[Changes to existing law are in shown in italics, bold, and strikethrough format]

18 U.S.C. § 1961(1).

(1) "racketeering activity" means … (B) any act which is indictable under any of the following provisions of title 18, United States Code: … section 1028 (relating to fraud and related activity in connection with identification documents), section 1029 (relating to fraud and related activity in connection with access devices), ***section 1030 (relating to fraud and related activity in connection with computers) if the act indictable under section 1030 is felonious,*** section 1084 (relating to the transmission of gambling information), section 1341 (relating to mail fraud), section 1343 (relating to wire fraud), …

18 U.S.C. § 1030. Fraud and Related Activity in Connection with Computers

(a) Whoever —

…

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information, ***or means of access*** through which a ***protected*** computer may be accessed without authorization~~, if —~~

~~(A) such trafficking affects interstate or foreign commerce~~; or

~~(B) such computer is used by or for the Government of the United States;~~

…

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided ***for the completed offense,*** in subsection (c) of this section.

(c)

(1)

~~(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and~~

~~(B)~~ a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under ~~subsection~~ ***paragraph*** (a)(1) of this section ~~which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph~~;

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than ~~one~~ ***three*** year***s***, or both, in the case of an offense under ~~subsection~~ ***paragraph*** (a)(2)~~, (a)(3), or (a)(6)~~ of this section ~~which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph~~;

(B) a fine under this title or imprisonment for not more than ~~5~~ ***ten*** years, or both, in the case of an offense under ~~subsection~~ ***paragraph*** (a)(2) ***of this section***, ~~or an attempt to commit an offense punishable under this subparagraph, if —~~

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; ~~and~~

~~(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;~~

(3)

~~(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and~~

~~(B)~~ ~~a fine under this title or imprisonment for not more than ten twenty years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;~~

a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under paragraph (a)(3) of this section;

(4)

~~(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of—~~

~~(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)—~~

~~(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting~~

~~from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;~~

~~(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;~~

~~(III) physical injury to any person;~~

~~(IV) a threat to public health or safety;~~

~~(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or~~

~~(VI) damage affecting 10 or more protected computers during any 1-year period; or~~

~~(ii) an attempt to commit an offense punishable under this subparagraph;~~

~~(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of—~~

~~(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or~~

~~(ii) an attempt to commit an offense punishable under this subparagraph;~~

~~(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of—~~

~~(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or~~

~~(ii) an attempt to commit an offense punishable under this subparagraph;~~

~~(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of—~~

~~(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or~~

~~(ii) an attempt to commit an offense punishable under this subparagraph;~~

~~(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;~~

~~(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or~~

~~(G) a fine under this title, imprisonment for not more than 1 year, or both, for—~~

~~(i) any other offense under subsection (a)(5); or~~

~~(ii) an attempt to commit an offense punishable under this subparagraph.~~

a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under paragraph (a)(4) of this section;

(5)

(A) Except as provided in subparagraph (D), a fine under this title, imprisonment for not more than twenty years, or both, in the case of an offense under subparagraph (a)(5)(A) of this section, if the offense caused—

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals;

(iii) physical injury to any person;

(iv) a threat to public health or safety;

(v) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(vi) damage affecting ten or more protected computers during any one-year period; or

(B) a fine under this title, imprisonment for not more than ten years, or both, in the case of an offense under subparagraph (a)(5)(B), if the offense caused a harm provided in (i) through (vi) of subparagraph (A) of this subsection; or

(C) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subparagraph (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(D) a fine under this title, imprisonment for not more than one year, or both, for any other offense under paragraph (a)(5);

(6) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under paragraph (a)(6) of this section;

(7) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under paragraph (a)(7) of this section.

…

(i) ***Criminal Forfeiture***

(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States—

(A) such person's interest in any ~~personal~~ property***, real or personal,*** that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from~~,~~ any ***gross*** proceeds***, or any property traceable to such property,*** that such person obtained~~,~~ directly or indirectly~~,~~ as a result of such violation.

(2) The criminal forfeiture of property under this subsection, ***including*** any seizure and disposition ***of the property*** ~~thereof~~, and any ***related*** judicial ***or administrative*** proceeding ~~in relation thereto~~, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) ***Civil Forfeiture***

(1) ~~For purposes of subsection (i), t~~***T***he following shall be subject to forfeiture to the United States and no property right shall exist in them:

(~~1~~***A***) Any ~~personal~~ property***, real or personal, that was*** used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(~~2~~***B***) Any property, real or personal, ~~which constitutes~~ ***constituting*** or ~~is~~ derived from ***any gross*** proceeds ***obtained directly or indirectly, or any property*** traceable to ***such property, as a result of the commission of*** any violation of this section, or a conspiracy to violate this section.

(2) Seizures and forfeitures under this subsection shall be governed by the provisions of chapter 46 of title 18, United States Code, relating to civil forfeitures, except that such duties as are imposed on the Secretary of the Treasury under the customs laws described in section 981(d) of title 18 shall be performed by such officers, agents, and other persons as may be designated for that purpose by the Secretary of Homeland Security or the Attorney General.

Legislative Language

Data Breach Notification

SEC. 1. DEFINITIONS.

In this Title, the following definitions shall apply:

(a) AFFILIATE.—The term "affiliate" means persons related by common ownership or by corporate control.
(b) BUSINESS ENTITY.—The term "business entity" means any organization, corporation, trust, partnership, sole proprietorship, unincorporated association, or venture established to make a profit, or nonprofit.
(c) DATA SYSTEM COMMUNICATION INFORMATION.—The term "data system communication information" means dialing, routing, addressing or signaling information that identifies the origin, direction, destination, processing, transmission, or termination of each communication initiated, attempted, or received.
(d) DATE AND TIME.—The term "date and time" includes the date and time and specification of the time zone offset from Coordinated Universal Time (UTC).
(e) INTERNET ADDRESS.—The term "Internet address" means an Internet Protocol address as specified by the Internet Protocol version 4 or 6 protocol, or any successor protocol or any unique number for a specific host on the Internet.
(f) SECURITY BREACH.—

(1) IN GENERAL.—The term "security breach" means a compromise of the security, confidentiality, or integrity of, or the loss of, computerized data that results in, or there is a reasonable basis to conclude has resulted in –

(A) the unauthorized acquisition of sensitive personally identifiable information; or
(B) access to sensitive personally identifiable information that is for an unauthorized purpose, or in excess of authorization.

(2) EXCLUSION.—The term "security breach" does not include any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION.—The term "sensitive personally identifiable information" means any information or compilation of information, in electronic or digital form that includes—

(1) an individual's first and last name or first initial and last name in combination with any two of the following data elements:
(A) Home address or telephone number;
(B) Mother's maiden name;
(C) Month, day, and year of birth;
(2) A non-truncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number;

(3) Unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation;
(4) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or
(5) Any combination of the following data elements:
    (A) An individual's first and last name or first initial and last name;
    (B) A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code; or
    (C) Any security code, access code, or password, or source code that could be used to generate such codes or passwords.
(6) MODIFIED DEFINITION BY RULEMAKING— The Federal Trade Commission may, by rule promulgated under section 553 of title 5, United States Code, amend the definition of `sensitive personally identifiable information' to the extent that such amendment will not unreasonably impede interstate commerce, and will accomplish the purposes of this Title. In amending the definition, the Federal Trade Commission may determine—
    (A) that any particular combinations of information are sensitive personally identifiable information, or
    (B) that any particular piece of information, on its own, is sensitive personally identifiable information.

SEC. 101. NOTICE TO INDIVIDUALS.

(a) In General.—Any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period shall, following the discovery of a security breach of such information, notify any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired, unless there is no reasonable risk of harm or fraud to such individual.

(b) Obligations of and to Owner or Licensee.—

(1) NOTICE TO OWNER OR LICENSEE.—Any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information that the business entity does not own or license shall notify the owner or licensee of the information following the discovery of a security breach involving such information, unless there is no reasonable risk of harm or fraud to such owner or licensee.

(2) NOTICE BY OWNER, LICENSEE OR OTHER DESIGNATED THIRD PARTY.—Nothing in this Title shall prevent or abrogate an agreement between a business entity required to give notice under this section and a designated third party, including an owner or licensee of the sensitive personally identifiable information subject to the security breach, to provide the notifications required under subsection (a).

(3) BUSINESS ENTITY RELIEVED FROM GIVING NOTICE.—A business entity obligated to give notice under subsection (a) shall be relieved of such obligation if an owner or licensee of the sensitive personally identifiable information subject to the security breach, or other designated third party, provides such notification.

(c) Timeliness of Notification.—

(1) IN GENERAL.—All notifications required under this section shall be made without unreasonable delay following the discovery by the business entity of a security breach. A business entity shall, upon the request of the Federal Trade Commission, provide records or other evidence of the notifications required under this Section.

(2) REASONABLE DELAY.—Reasonable delay under this subsection shall not exceed 60 days, except as provided in subsection 101(d) or unless the business entity seeking additional time demonstrates to the Federal Trade Commission that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to an entity designated by the Secretary of Homeland Security to receive reports and information about information security incidents, threats, and vulnerabilities when required. If the Federal Trade Commission determines that additional delay is necessary the agency may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing.

(3) BURDEN OF PRODUCTION.— If a business entity requires additional time under paragraph (2), it shall provide the Federal Trade Commission with records or other evidence of the reasons necessitating delay of notification.

(d) Delay of Notification Authorized for Law Enforcement or National Security Purposes.—

(1) IN GENERAL.—If a Federal law enforcement agency determines that the notification required under this section would impede a criminal investigation or national security activity, such notification shall be delayed upon written notice from such Federal law enforcement agency to the business entity that experienced the breach.

(2) EXTENDED DELAY OF NOTIFICATION.—If the notification required under subsection (a) is delayed pursuant to paragraph (1), a business entity shall give notice 30 days after the day such delay was invoked unless a Federal law enforcement agency provides written notification that further delay is necessary. Written notifications for further delay shall specify the period of delay to which they apply.

(3) IMMUNITY.—No non-constitutional cause of action shall lie in any court against any federal agency for acts relating to the delay of notification for law enforcement or national security purposes under this Title.

SEC. 102. EXEMPTIONS FROM NOTICE TO INDIVIDUALS.

(a) Exemption for National Security and Law Enforcement. –

(1) IN GENERAL.— If the United States Secret Service or Federal Bureau of Investigation determines that notification of the security breach could be expected to reveal sensitive sources and methods or similarly impede the ability of the agency to conduct law enforcement investigations, or if the Federal Bureau of Investigation determines that notification of the security breach could be expected to cause damage to the national security, notification under this section is not required.

(2) IMMUNITY.—No non-constitutional cause of action shall lie in any court against any federal agency for acts relating to the exemption from notification for law enforcement or national security purposes under this Title.

(b) Safe Harbor.—

(1) IN GENERAL.— A business entity will be exempt from the notice requirements under section 101, if—

(A) a risk assessment conducted by or on behalf of the business entity concludes that there is no reasonable risk that a security breach has resulted in, or will result in, harm to the individuals whose sensitive personally identifiable information was subject to the security breach. If the data at issue was rendered unusable, unreadable, or indecipherable through a security technology or methodology generally accepted by experts in the field of information security, there shall be a presumption that no reasonable risk exists. Any such presumption shall be rebuttable by facts demonstrating that the security technologies or methodologies in a specific case have been, or are reasonably likely to have been, compromised; and

(B) without unreasonable delay, but not later than 45 days after the discovery of a security breach, unless extended by the Federal Trade Commission, the business entity notifies the Federal Trade Commission, in writing, of—

(i) the results of the risk assessment; and

(ii) its decision to invoke the risk assessment exemption.

(2) RISK ASSESSMENTS.—

(A) Failure to conduct the risk assessment in a reasonable manner or according to standards generally accepted by experts in the field of information security shall constitute a violation of this section.

(B) A risk assessment must include logging data, as applicable and to the extent available, for a period of at least six months prior to submitting the risk assessment—

(1) for each communication or attempted communication with a database or data system containing sensitive personally identifiable information, the

data system communication information for the communication or attempted communication, including any Internet addresses, and the date and time associated with the communication or attempted communication; and

(2) all log-in information associated with databases or data systems containing sensitive personally identifiable information, including both administrator and user log-in information.

(C) Submitting a risk assessment containing fraudulent or deliberately misleading information shall constitute a violation of this section.

(c) Financial Fraud Prevention Exemption.—

(1) IN GENERAL.—A business entity will be exempt from the notice requirement under section 101 if the business entity utilizes or participates in a security program that—

(A) effectively blocks the use of the sensitive personally identifiable information to initiate unauthorized financial transactions before they are charged to the account of the individual; and

(B) provides for notice to affected individuals after a security breach that has resulted in fraud or unauthorized transactions.

(2) LIMITATION.—The exemption in paragraph (1) does not apply if the information subject to the security breach includes the individual's first and last name or any other type of sensitive personally identifiable information other than a credit card number or credit card security code.

SEC. 103. METHODS OF NOTICE TO INDIVIDUALS.

A business entity shall be in compliance with section 101 if it provides both:

(1) INDIVIDUAL NOTICE.—Notice to individuals by 1 of the following means:

(A) Written notification to the last known home mailing address of the individual in the records of the business entity.

(B) Telephone notice to the individual personally.

(C) E-mail notice, if the individual has consented to receive such notice and the notice is consistent with the provisions permitting electronic transmission of notices under section 101 of the Electronic Signatures in Global and National Commerce Act (15 U.S.C. 7001).

(2) MEDIA NOTICE.— If the number of residents of a State whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by

an unauthorized person exceeds 5,000, notice to media reasonably calculated to reach such individuals, such as major media outlets serving a State or jurisdiction.

SEC. 104. CONTENT OF NOTICE TO INDIVIDUALS.

(a) In General.—Regardless of the method by which notice is provided to individuals under section 103, such notice shall include, to the extent possible—

(1) a description of the categories of sensitive personally identifiable information that was, or is reasonably believed to have been, accessed or acquired by an unauthorized person;

(2) a toll-free number—

(A) that the individual may use to contact the business entity, or the agent of the business entity; and

(B) from which the individual may learn what types of sensitive personally identifiable information the business entity maintained about that individual; and

(3) the toll-free contact telephone numbers and addresses for the major credit reporting agencies and the Federal Trade Commission.

(b) Direct Business Relationship. —Regardless of whether the business entity or a designated third party provides notice pursuant to Section 101(b) of this Act, notice shall provide notice of the business entity that has a direct business relationship with the individual.

(c) Additional Content.—Notwithstanding section 109, a State may require that a notice under subsection (a) shall also include information regarding victim protection assistance provided for by that State.

SEC. 105. COORDINATION OF NOTIFICATION WITH CREDIT REPORTING AGENCIES.

(a) If a business entity is required to provide notification to more than 5,000 individuals under section 101, the business entity shall also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis (as defined in section 603(p) of the Fair Credit Reporting Act (15 U.S.C. 1681a(p)) of the timing and distribution of the notices. Such notice shall be given to the consumer credit reporting agencies without unreasonable delay and, if it will not delay notice to the affected individuals, prior to the distribution of notices to the affected individuals.

(b) Reasonable delay under subsection (a) shall not exceed 60 days, except as provided in section 101(d) and 102(a) or unless the business entity providing notice can demonstrate to the Federal Trade Commission that additional time is reasonably necessary to determine the scope of the security breach, prevent further disclosures, conduct the risk assessment, restore the reasonable integrity of the data system, and provide notice to an entity designated by the

Secretary of Homeland Security to receive reports and information about information security incidents, threats, and vulnerabilities when required. If the Federal Trade Commission determines that additional delay is necessary the agency may extend the time period for notification for additional periods of up to 30 days each. Any such extension shall be provided in writing.

SEC. 106. NOTICE FOR LAW ENFORCEMENT AND OTHER PURPOSES.

(a) Notice to Law Enforcement and National Security Authorities.—Any business entity shall notify an entity designated by the Secretary of Homeland Security to receive reports and information about information security incidents, threats, and vulnerabilities, and such agency shall promptly notify and provide that same information to the United States Secret Service, the Federal Bureau of Investigation, and the Federal Trade Commission for civil law enforcement purposes, and shall make it available as appropriate to other federal agencies for law enforcement, national security, or computer security purposes, if—

(1) the number of individuals whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person exceeds 5000;

(2) the security breach involves a database, networked or integrated databases, or other data system containing the sensitive personally identifiable information of more than 500,000 individuals nationwide;

(3) the security breach involves databases owned by the Federal Government; or

(4) the security breach involves primarily sensitive personally identifiable information of individuals known to the business entity to be employees and contractors of the Federal Government involved in national security or law enforcement.

(b) FTC Rulemaking. – Not later one year after the date of the enactment of this Act, in consultation with the Attorney General and the Secretary of Homeland Security, the Federal Trade Commission shall promulgate regulations defining what information notifications under subsection (a) must contain. In addition, in consultation with the Attorney General, the Federal Trade Commission shall promulgate regulations, as necessary, under section 553 of title 5, United States Code, to adjust the thresholds for notice to law enforcement and national security authorities under subsection (a) and to facilitate the purposes of this section.

(c) Timing of Notice.—The notice required under this section shall be provided as promptly as possible, but must occur 72 hours before notification of an individual pursuant to section 101 or 10 days after discovery of the events requiring notice, whichever comes first.

SEC. 107. ENFORCEMENT.

(a) Unfair or deceptive acts or practices.—Compliance with the requirements imposed under this Title shall be enforced under the Federal Trade Commission Act [15 U.S.C. 41 et seq.] by the

Federal Trade Commission with respect to business entities subject to this Act. For the purpose of the exercise by the Federal Trade Commission of its functions and powers under the Federal Trade Commission Act, a violation of any requirement or prohibition imposed under this Title shall constitute an unfair or deceptive act or practice in commerce in violation of a regulation under section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C.57a(a)(1)(B)) regarding unfair or deceptive acts or practices and shall be subject to enforcement by the Federal Trade Commission under that Act with respect to any business entity, irrespective of whether that business entity is engaged in commerce or meets any other jurisdictional tests in the Federal Trade Commission Act. All of the functions and powers of the Federal Trade Commission under the Federal Trade Commission Act are available to the Commission to enforce compliance by any person with the requirements imposed under this Title. Where enforcement relates to customer proprietary network information, enforcement actions by the Federal Trade Commission will be coordinated with the Federal Communications Commission.

(b) Before opening an investigation, the Federal Trade Commission must consult with the Attorney General. The Federal Trade Commission may initiate investigations under this subsection unless the Attorney General determines that such an investigation would impede an ongoing criminal investigation or national security activity.

(c) Rulemaking. - The Federal Trade Commission may, in addition to the specific rulemakings required or authorized by this Title, issue such other regulations as it determines to be necessary to carry out this Title. All regulations promulgated under this Act shall be issued in accordance with section 553 of title 5, United States Code. Where regulations relate to customer proprietary network information, the promulgation of such regulations will be coordinated with the Federal Communications Commission.

SEC. 108. ENFORCEMENT BY STATE ATTORNEYS GENERAL.

(a) In General.—

(1) CIVIL ACTIONS.—In any case in which the attorney general of a State or any State or local law enforcement agency authorized by the State attorney general or by State statute to prosecute violations of consumer protection law, has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of a business entity in a practice that is prohibited under this Title or the failure to meet a requirement imposed under this Title, the attorney general of the State or the State or local law enforcement agency on behalf of the residents of the agency's jurisdiction, may bring a civil action on behalf of the residents of the State or jurisdiction in a district court of the United States of appropriate jurisdiction or any other court of competent jurisdiction, including a State court, to—

(A) enjoin that practice;

(B) enforce compliance with this Title; or

(C) civil penalties of not more than $1,000 per day per individual whose sensitive personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $1,000,000 per violation unless such conduct is found to be willful or intentional.

(2) NOTICE.— Before filing an action under paragraph (1), the attorney general of the State or the State or local law enforcement agency shall provide to the Attorney General and the Federal Trade Commission—

(i) written notice of the action; and

(ii) a copy of the complaint for the action. Such actions shall not be filed if the Attorney General certifies that the filing would impede a criminal investigation or national security activity.

(b) Federal Proceedings.—Upon receiving notice under subsection (a)(2), the Federal Trade Commission shall have the right to—

(1) move to stay the action, pending the final disposition of a pending Federal proceeding or action;

(2) initiate an action in the appropriate United States district court under section 107 and move to consolidate all pending actions, including State actions, in such court;

(3) intervene in an action brought under subsection (a)(2); and

(4) file petitions for appeal.

(c) Pending Proceedings.—If the Federal Trade Commission has instituted a proceeding or action for a violation of this Title or any regulations thereunder, no attorney general of a State or State or local law enforcement agency may, during the pendency of such proceeding or action, bring an action under this Title against any defendant named in such civil action for any violation that is alleged in that proceeding or action.

(d) Construction.—For purposes of bringing any civil action under subsection (a), nothing in this Title regarding notification shall be construed to prevent an attorney general of a State or a State or local law enforcement agency from exercising the powers conferred on such attorney general by the laws of that State to—

(1) conduct investigations;

(2) administer oaths or affirmations; or

(3) compel the attendance of witnesses or the production of documentary and other evidence.

(e) Venue; Service of Process.—

(1) VENUE.—Any action brought under subsection (a) may be brought in—

(A) the district court of the United States that meets applicable requirements relating to venue under section 1391 of title 28, United States Code; or

(B) another court of competent jurisdiction.

(2) SERVICE OF PROCESS.—In an action brought under subsection (a), process may be served in any district in which the defendant—

(A) is an inhabitant; or

(B) may be found.

(f) No Private Cause of Action.—Nothing in this Title establishes a private cause of action against a business entity for violation of any provision of this Title.

SEC. 109. EFFECT ON FEDERAL AND STATE LAW.

The provisions of this Title shall supersede any provision of the law of any State, or a political subdivision thereof, relating to notification by a business entity engaged in interstate commerce of a security breach of computerized data, except as provided in section 104(c).

SEC. 110. REPORTING ON RISK ASSESSMENT.

(a) The United States Secret Service and Federal Bureau of Investigation shall report to Congress not later than 18 months after the date of enactment of this Title, and upon the request by Congress thereafter, on the number and nature of security breaches subject to the national security and law enforcement exemptions under section 102(a).

(b) The Federal Trade Commission shall report to Congress not later than 18 months after the date of enactment of this Title, and upon the request of Congress thereafter, on the number and nature of the security breaches described in the notices filed by those business entities invoking the risk assessment exemption under section 102(b) and the response of the Federal Trade Commission to such notices.

SEC. 111. EXCLUDED BUSINESS ENTITIES.

Nothing in this Act shall apply to

(a) Business entities to the extent that they act as covered entities and business associates subject to the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 17932), including the data breach notification requirements and implementing regulations of that Act; and

(b) Business entities to the extent that they act as vendors of personal health records and third party service providers subject to the Health Information Technology for Economic and Clinical Health Act (42 U.S.C. § 17937), including the data breach notification requirements and implementing regulations of that Act.

SEC. 112. EFFECTIVE DATE.

This Title shall take effect on the expiration of the date which is 90 days after the date of enactment.

Legislative Language

SECTION 1. DEPARTMENT OF HOMELAND SECURITY CYBERSECURITY AUTHORITY.—

Title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.) is amended—

(a) in section 201(c) by striking "or the Assistant Secretary for Infrastructure Protection, as appropriate," and inserting "and the Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department, as appropriate."; and

(b) by adding at the end the following:

‘‘**Subtitle E – Cybersecurity Programs**

‘‘**SEC. 241. SHORT TITLE. This Act may be cited as the "Department of Homeland Security Cybersecurity Authority and Information Sharing Act of 2011."**

‘‘**SEC. 242. DEFINITIONS.**

‘‘In this subtitle:

‘‘ (1) AGENCY. —The term "agency" has the meaning given that term in section 3502(1) of title 44, as amended.

‘‘ (2) COMMUNICATION.—The term "communication" means any electronic communication or wire communication transiting to or from or stored on a federal system or critical information infrastructure.

‘‘ (3) COUNTERMEASURE.—The term "countermeasure" means automated actions with defensive intent to modify or block data packets associated with electronic or wire communications, internet traffic, program code, or other system traffic transiting to or from or stored on an information system for the purpose of protecting the information system from cybersecurity threats, conducted on an information system or information systems owned or operated by or on behalf of the party to be protected or operated by a private entity acting as a provider of electronic communication services, remote computing services, or cybersecurity services to the party to be protected.

‘‘ (4) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given that term in section 5195c(e) of title 42.

‘‘ (5) CRITICAL INFORMATION INFRASTRUCTURE.—The term "critical information infrastructure" means any physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice or video that is—

‘‘ (A) vital to the functioning of critical infrastructure;

‘‘ (B) so vital to the United States that the incapacity or destruction of such systems would have a debilitating impact on national security, national economic security, or national public health or safety; or

‘‘ (C) owned or operated by or on behalf of a state, local, tribal, or territorial government entity.

“ Except that the term “critical information infrastructure” shall not include agency information systems, including federal systems, national security systems, or information systems under the control of the Department of Defense.
‘‘ (6) CYBERSECURITY SERVICES.—The term “cybersecurity services” means products, goods, or services intended to detect or prevent activity intended to result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system.
‘‘ (7) CYBERSECURITY THREAT.— The term “cybersecurity threat” means any action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system.
‘‘ (8) ELECTRONIC COMMUNICATION.— The term “electronic communication” has the meaning given that term in section 2510 of title 18.
‘‘ (9) ELECTRONIC COMMUNICATION SERVICE.—The term “electronic communication service” has the meaning given that term in section 2510 of title 18.
‘‘ (10) FEDERAL SYSTEMS.—The term “federal systems” means all information systems owned, operated, leased, or otherwise controlled by an agency, except for national security systems or those information systems under the control of the Department of Defense.
‘‘ (11) INCIDENT.—The term “incident” has the meaning given that term in Chapter 35 of title 44, as amended.
‘‘ (12) INFORMATION SECURITY.—The term “information security” has the meaning given that term in section 3551 of title 44.
‘‘ (13) INFORMATION SYSTEM.—The term “information system” has the meaning given that term in section 3502(8) of title 44.
‘‘ (14) GOVERNMENTAL ENTITY.—The term “governmental entity” has the meaning given that term in section 2711 of title 18.
‘‘ (15) NATIONAL SECURITY SYSTEM.—The term “national security system” has the meaning given that term in section 3552 of title 44.
‘‘ (16) PRIVATE ENTITY.—The term “private entity” means any entity other than a governmental entity as defined in section 2711(4) of title 18.
‘‘ (17) PROTECT.—The term “protect” means those actions undertaken to secure, defend, or reduce the vulnerabilities of an information system, mitigate cybersecurity threats, or otherwise enhance information security or the resiliency of information systems or assets.
‘‘ (18) WIRE COMMUNICATION.—The term “wire communication” has the meaning given that term in section 2510 of title 18.

‘‘**SEC. 243. ENHANCEMENT OF NATIONAL CYBERSECURITY AND CYBER INCIDENT RESPONSE.**
‘‘ (a) IN GENERAL.—The Secretary shall engage in cybersecurity, and other infrastructure protection activities under this title, to support the functioning of federal systems and critical information infrastructure in the interests of national security, national economic security, and national public health and safety.

‘‘ (b) APPROACH.—In carrying out the responsibilities under this subtitle and section 201 of this Act, the Secretary, as appropriate, shall develop and maintain risk-informed approaches that—

‘‘ (1) improve, on an ongoing basis, the information security of federal systems and critical information infrastructure, with particular attention to addressing high consequence risks to national interests;

‘‘ (2) consider the economic competitiveness of United States industry, including the information and communications industries;

‘‘ (3) promote the development and implementation of technical capabilities in support of national cybersecurity goals;

‘‘ (4) minimize the impact of the activities carried out under this subtitle on privacy and civil liberties consistent with section 248(a);

‘‘ (5) promote greater research, innovation, training, education, outreach, public awareness, and investment in cybersecurity; and

‘‘ (6) foster the development of secondary markets and widespread adoption of cybersecurity technology by critical information infrastructure.

‘‘ (c) AUTHORITY AND RESPONSIBILITY TO CONDUCT CYBERSECURITY ACTIVITIES.—To protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against incidents involving such systems and infrastructure, the Secretary shall, in accordance with this subtitle—

‘‘ (1) create appropriate programs to carry out the purpose and responsibilities under this subtitle;

‘‘ (2) develop and conduct risk assessments for federal systems and, upon request, critical information infrastructure in consultation with the heads of other agencies or governmental and private entities that own and operate such systems and infrastructure, that may include threat, vulnerability, and impact assessments and penetration testing;

‘‘ (3) foster the development, in conjunction with other governmental entities and the private sector, of essential information security technologies and capabilities for protecting federal systems and critical information infrastructure, including comprehensive protective capabilities and other technological solutions;

‘‘ (4) acquire, integrate, and facilitate the adoption of new cybersecurity technologies and practices to keep pace with emerging cybersecurity threats and developments, including through research and development, technology leasing arrangements, technical service agreements, and making such technologies available to governmental and private entities that own or operate critical information infrastructure, with or without reimbursement, as necessary to accomplish the purpose of this section;

‘‘ (5) designate and maintain a center to serve as a focal point within the federal government for cybersecurity with responsibilities that include the protection of federal systems and critical information infrastructure and the coordination of cyber incident response and that will—

‘‘ (A) facilitate information sharing, interactions and collaborations among and between agencies; State, local, tribal and territorial governments; the private sector; academia and international partners;

‘‘ (B) work with appropriate agencies; State, local, tribal and territorial governments; the private sector; academia; and international partners to prevent and respond to cybersecurity threats and incidents involving federal systems and critical information infrastructure pursuant to the national cyber incident response plan and supporting plans developed in accordance with paragraph (9);

‘‘ (C) disseminate timely and actionable cybersecurity threat, vulnerability, mitigation and warning information, including alerts, advisories, indicators, signatures, and mitigation and response measures, to improve the security and protection of federal systems and critical information infrastructure;

‘‘ (D) integrate information from federal government and non-federal network operation centers and security operations centers to provide situational awareness of the Nation’s information security posture and foster information security collaboration among information system owners and operators;

‘‘ (E) compile and analyze information about risks and incidents that threaten federal systems and critical information infrastructure, including information voluntarily submitted in accordance with section 245 or otherwise in accordance with applicable laws; and

‘‘ (F) provide incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to heads of agencies and, upon request, governmental or private entities that own or operate critical information infrastructure;

‘‘ (6) assist in national efforts to mitigate communications and information technology supply chain vulnerabilities to enhance the security and the resiliency of federal systems and critical information infrastructure;

‘‘ (7) develop and lead a nationwide awareness and outreach effort to educate members of the public about —

‘‘ (A) the importance of cybersecurity;

‘‘ (B) ways to help promote cybersecurity best practices at home and in the workplace;

‘‘ (C) training opportunities to support the development of an effective national cybersecurity workforce; and

“ (D) educational paths to cybersecurity professions;

‘‘ (8) establish in cooperation with the Director of the National Institute of Standards and Technology benchmarks and guidelines for making the critical information infrastructure more secure at a fundamental level, including through automation, interoperability, and privacy-enhancing authentication;

‘‘ (9) develop a national cybersecurity incident response plan and supporting cyber incident response and restoration plans, in collaboration with other relevant agencies; owners and operators of critical information infrastructure; sector coordinating councils; state, local, territorial, and tribal governments; and relevant non-governmental organizations and based on applicable law, that describe the specific roles and responsibilities of governmental and private entities during cyber incidents;

‘‘ (10) develop and conduct exercises, simulations, and other activities designed to support the national response to cybersecurity threats and incidents and evaluate the national cyber incident response plan and supporting plans developed in accordance with paragraph (9); and

‘‘ (11) take such other lawful action as may be necessary and appropriate to accomplish the requirements of this section.

‘‘ (d) COORDINATION AND COOPERATION. —

‘‘ (1) In carrying out the cybersecurity activities under this section, the Secretary shall coordinate, as appropriate, with—

‘‘ (A) the head of any relevant agency or entity;

‘‘ (B) representatives of State, local, tribal, territorial, and foreign governments;

‘‘ (C) the private sector, including owners and operators of critical information infrastructure;

‘‘ (D) academia; and

‘‘ (E) international organizations and foreign partners.

‘‘ (2) The Secretary shall coordinate the activities undertaken by agencies to protect federal systems and critical information infrastructure and prepare the nation to respond to, recover from, and mitigate against risk of incidents involving such systems and infrastructure.

‘‘ (3) The Secretary shall ensure that the Department’s cybersecurity activities under this subtitle are coordinated with all other infrastructure protection and cyber-related programs and activities of the Department, including those of any intelligence or law enforcement components or entities within the Department.

“(e) NO RIGHT OR BENEFIT. – The provision of assistance or information to governmental or private entities that own or operate critical information infrastructure under this section shall be at the discretion of the Secretary. The provision of certain assistance or information to one governmental or private entity pursuant to this section shall not create a right or benefit, substantive or procedural, to similar assistance or information for any other governmental or private entity.

“(f) SAVINGS CLAUSE. —Nothing in this subtitle shall be interpreted to alter or amend the law enforcement or intelligence authorities of any agency.

‘‘**SEC. 244. NATIONAL CYBERSECURITY PROTECTION PROGRAM.—**

‘‘ (a) In furtherance of the responsibilities assigned under section 243, the Secretary shall carry out a cybersecurity program to protect federal systems from cybersecurity threats that may include—

‘‘ (1) operating consolidated intrusion detection, prevention, or other protective capabilities and the use of associated countermeasures for the purpose of protecting federal systems from cybersecurity threats;

‘‘ (2) conducting the risk assessments, including threat, vulnerability, and impact assessments and penetration testing, on federal systems consistent with section 243(c)(2);

“ (3) providing incident detection, analysis, mitigation, and response information and remote or on-site technical assistance to federal system owners and operators consistent with section 243(c)(5)(F);

‘‘ (4) ensuring common situational awareness of cybersecurity threats and incidents across federal systems to support the protection of federal systems and the operation and defense of external access points across all federal systems;
‘‘ (5) directing, pursuant to section 249, that agencies that own or operate a federal system take action with respect to the operation of such system for the purpose of protecting that system or mitigating a cybersecurity threat;
‘‘ (6) discharging the responsibilities for federal information security set forth in chapter 35 of title 44, including the establishment of reporting requirements regarding incidents that impair the adequate security of agency information systems and designation of an entity to receive reports and information about agency information security incidents, threats, and vulnerabilities affecting agency information systems; and
‘‘ (7) testing and evaluating, consistent with applicable law, information security improvements within the Department.

‘‘ (b) While carrying out the program authorized in subsection (a), the Secretary is authorized, notwithstanding any other provision of law and consistent with section 248(a), to acquire, intercept, retain, use, and disclose communications and other system traffic that are transiting to or from or stored on federal systems and to deploy countermeasures with regard to such communications and system traffic provided that the Secretary certifies that—

‘‘ (1) such acquisitions, interceptions, and countermeasures are reasonably necessary for the purpose of protecting federal systems from cybersecurity threats;
‘‘ (2) the content of communications will be collected and retained only when the communication is associated with a known or reasonably suspected cybersecurity threat, and communications and system traffic will not be subject to the operation of a countermeasure unless associated with such threats;
‘‘ (3) information obtained pursuant to activities authorized under this subsection will only be retained, used or disclosed to protect federal systems from cybersecurity threats, mitigate against such threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed;
‘‘ (4) the communications and system traffic to be acquired, intercepted, retained, used or disclosed are transiting to or from or stored on a federal system;
‘‘ (5) notice has been provided to users of federal systems concerning the potential for acquisition, interception, retention, use, and disclosure of communications and other system traffic; and
‘‘ (6) the cybersecurity program, including the acquisition, interception, retention, use, and disclosure of communications and other system traffic, is implemented consistent with section 248(a).

‘‘ (c) Agencies are authorized to permit the Secretary to acquire, intercept, retain, use, and disclose communications, system traffic, records, or other information transiting to or from or stored on a federal system, notwithstanding any other provision of law, for the purpose of protecting federal systems from cybersecurity threats or mitigating such threats in connection with the implementation of the cybersecurity program authorized by this section.

‘‘ (d) Any certification issued under subsection (b) may be valid for up to one year. The Secretary may extend any such authorization for additional periods of up to one year in the same manner required for the original certification.
‘‘ (e) The Secretary may request and obtain the assistance of private entities that provide electronic communications or cybersecurity services to implement this program. The Secretary shall ensure, by written agreement, that such assistance is conducted consistent with section 248(a).
‘‘ (f) Agencies shall implement this program in accordance with the Secretary’s certification and the requirements of this subtitle. The acquisition, interception, retention, use, or disclosure of communications, record, system traffic and other information by officers, employees, or agents of any agency, except as authorized in subsection (b) and (c) and in accordance with the Secretary’s certification or otherwise in accordance with law shall be a violation of this subtitle.
‘‘ (g) In implementing the cybersecurity program authorized in subsection (a) and activities authorized in subsection (b), the Secretary shall coordinate with heads of appropriate agencies, including those responsible for federal systems to accomplish the purposes of this section consistent with agency mission requirements.

‘‘ **SEC. 245. VOLUNTARY DISCLOSURE OF CYBERSECURITY INFORMATION.—**
‘‘ (a)(1) A non-federal governmental or private entity, or any officer, employee, or agent thereof, that lawfully intercepts, acquires, or otherwise obtains or possesses any communication, record, or other information, notwithstanding any other provision of law and consistent with section 248(a), may disclose that communication, record, or other information to the cybersecurity center designated by the Secretary under section 243(c)(5) for the purpose of protecting an information system from cybersecurity threats or mitigating such threats provided that reasonable efforts are undertaken to remove information that can be used to identify specific persons unrelated to the cybersecurity threat before any disclosure.

> ‘‘ (2) An agency, or any officer, employee, or agent thereof, that lawfully intercepts, acquires, or otherwise obtains or possesses any communication, record, or other information from its electronic communications system, notwithstanding any other provision of law and consistent with section 248(b), may disclose that communication, record, or other information to—
>
> > ‘‘ (A) another component, officer, employee, or agent of that agency with cybersecurity responsibilities;
> > ‘‘ (B) the cybersecurity center designated by the Secretary under section 243(c)(5); or
> > ‘‘ (C) a private entity that is acting as a provider of electronic communication services, remote computing service, or cybersecurity services to the agency
>
> for the purpose of protecting an agency information system from cybersecurity threats or mitigating cybersecurity threats.

‘‘ (b)(1) The Department may only use, retain or further disclose information to appropriate governmental and private entities obtained pursuant to this section, consistent with section 248(a), in order to protect information systems from cybersecurity threats,

mitigate cybersecurity threats, or, with the approval of the Attorney General, to law enforcement entities when the information is evidence of a crime which has been, is being, or is about to be committed.

‘‘ (2) Agencies receiving communications, records or other information from the Department pursuant to paragraph (1) shall only use or retain such communications, records or other information consistent with section 248(b) in order to protect agency information systems from cybersecurity threats, mitigate cybersecurity threats, or, with the approval of the Attorney General, for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed.

‘‘ (c) Agencies shall ensure, by written agreement, that when disclosing communications, records or other information to non-federal governmental or private entities under this section, such non-federal governmental or private entities use or retain such communications, records or other information consistent with section 248(a) and for the purpose of protecting information systems from cybersecurity threats, mitigating cybersecurity threats, or for law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed. The Attorney General shall approve any disclosures for law enforcement purposes prior to disclosure.

‘‘ (d) Nothing in this section shall limit or prohibit otherwise lawful disclosures of communications, records, or information by a private entity to the Department or any other governmental or private entity not conducted under this section.

‘‘ (e) Nothing in this section permits the unauthorized disclosure of information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations; any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954; information related to intelligence sources and methods; or information that is specifically subject to a court order or a certification, directive or other authorization by the Attorney General precluding such disclosure.

‘‘ (f) Any communication, record, or other information disclosed by a State or local government entity or a private entity to the Department pursuant to subsection (a) shall be exempt from disclosure under section 552(b)(3) of title 5 or any comparable state law. Such communications, records, and other information shall be treated as voluntarily shared information under section 552 of title 5 and any comparable state law.

‘‘ (g) The disclosure or use of communications under this section in a manner not authorized in this section shall be a violation of this subtitle.

SEC. 246. LIMITATION ON LIABILITY AND GOOD FAITH DEFENSE FOR CYBERSECURITY ACTIVITIES.—

‘‘ (a) No civil or criminal cause of action shall lie or be maintained in any Federal or State court against any non-federal governmental or private entity, or any officer, employee, or agent thereof, for—

‘‘ (1) the disclosure of any communication, record, or other information authorized by this subtitle; or

‘‘ (2) any assistance provided to the Department pursuant to section 244(e),

and any such action shall be dismissed promptly.

‘‘ (b) Where a civil or criminal cause of action is not barred under subsection (a), a good faith reliance by any person on a legislative authorization, a statutory authorization, or a good faith determination that this subtitle permitted the conduct complained of, is a complete defense against any civil or criminal action brought under this subtitle or any other law.

SEC. 247. FEDERAL PREEMPTION, EXCLUSIVITY, AND LAW ENFORCEMENT ACTIVITIES.—

‘‘ (a) This subtitle supersedes any statute of a State or political subdivision of a State that restricts or otherwise expressly regulates the acquisition, interception, retention, use or disclosure of communications, records, or other information by private entities or governmental entities to the extent such statute is inconsistent with this subtitle.

‘‘ (b) Section 244(b) shall constitute an additional exclusive means for the domestic interception of wire or electronic communications, in accordance with section 1812(b) of Title 50.

‘‘ (c) This subtitle does not authorize the Secretary to engage in law enforcement or intelligence activities that the Department is not otherwise authorized to conduct under existing law.

SEC. 248. PRIVACY AND CIVIL LIBERTIES; OVERSIGHT; PENALTIES FOR MISUSE.—

‘‘ (a) In consultation with privacy and civil liberties experts, the Secretary shall develop and periodically review policies and procedures governing the acquisition, interception, retention, use, and disclosure of communications, records, system traffic or other information associated with specific persons by officers, employees, and agents of the Department obtained in connection with activities authorized in this subtitle. The policies and procedures developed under this subsection shall be reviewed and approved by the Attorney General. Such policies and procedures shall—

‘‘ (1) minimize the impact on privacy and civil liberties, consistent with the need to protect federal systems and critical information infrastructure from cybersecurity threats and mitigate cybersecurity threats;

‘‘ (2) reasonably limit the acquisition, interception, retention, use and disclosure of communications, records, system traffic or other information associated with specific persons consistent with the need to carry out the responsibilities of this subtitle, including establishing a process for the timely destruction on recognition of communications, records, system traffic or other information that is acquired or intercepted pursuant to this section that does not reasonably appear to be related to protecting federal systems and critical information infrastructure from cybersecurity threats and mitigating cybersecurity threats;

‘‘ (3) include requirements to safeguard communications, records, system traffic or other information that can be used to identify specific persons from unauthorized access or acquisition; and

“(4) protect the confidentiality of disclosed communications, records, system traffic or other information associated with specific persons to the greatest extent practicable and require recipients to be informed that the communications, records, system traffic or other information disclosed may only be used for protecting information

systems against cybersecurity threats, mitigating against cybersecurity threats, or law enforcement purposes when the information is evidence of a crime which has been, is being, or is about to be committed, as specified by the Secretary.

‘‘ (b) In consultation with privacy and civil liberties experts, and consistent with the requirements of subsection (a), the head of each agency shall develop and periodically review policies and procedures governing the acquisition, interception, retention, use, and disclosure of communications, records, system traffic or other information associated with specific persons by officers, employees, and agents of the agency obtained or disclosed in connection with activities authorized in this subtitle. The policies and procedures developed under this subsection shall be reviewed and approved by the Attorney General within one year of the effective date of this Act.

‘‘ (c) The head of each agency shall establish a program to monitor and oversee compliance with the policies and procedures issued under subsection (a) or (b) respectively. The head of the agency shall promptly notify the Attorney General of significant violations of such policies and procedures, and shall provide the Attorney General with any information relevant to the violation that the Attorney General requires.

‘‘ (d) The policies and procedures under subsection (a) or (b) and any amendments thereto shall be provided to the Congress.

‘‘ (e) On an annual basis, the Chief Privacy and Civil Liberties Officer of the Department of Justice and the Department, in consultation with the most senior privacy and civil liberties officer or officers of appropriate agencies shall submit a joint report to the Congress assessing the privacy and civil liberties impact of the governmental activities conducted pursuant to this subtitle.

‘‘ (f) Two years after enactment of this provision, the Privacy and Civil Liberties Oversight Board shall submit a report to the Congress and the President providing its assessment of the privacy and civil liberties impact of the government’s activities under this subtitle and recommending improvements to or modifications of the law to address privacy and civil liberties concerns.

‘‘ (g) No communications, records, system traffic or other information acquired or collected pursuant to this subtitle may be used, retained or disclosed by governmental or private entities except as authorized under this subtitle.

‘‘ (h) No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subtitle shall lose its privileged character.

‘‘ (i) The heads of agencies shall develop and enforce appropriate sanctions for officers, employees or agents of the agency who conduct activities under this subtitle—

‘‘ (1) outside the normal course of their specified duties;

‘‘ (2) in a manner inconsistent with the discharge of the agency’s responsibilities; or

‘‘ (3) in contravention of policies and procedures under subsection (a) or (b) respectively.

‘‘ (j) Any person who knowingly and willfully violates restrictions under this subtitle with respect to acquisition, interception, use, retention or disclosure of communications, records, system traffic or other information, or the related procedures established pursuant to subsection (a) or (b) shall be guilty of a misdemeanor and fined not more than $5,000 per incident.

“SEC. 249. REQUIRED SECURITY ACTION.—

“ (a) In response to a known or reasonably suspected cybersecurity threat or incident, the Secretary may direct officials of agencies that own or operate a federal system to take any lawful action with respect to the operation of such system for the purpose of protecting that system from or mitigating a cybersecurity threat. The Secretary shall—

“ (1) establish, in coordination with the Director of the Office of Management and Budget, procedures governing the circumstances under which such directive may be issued under this section, including—

“ (A) thresholds and other criteria;

“ (B) privacy and civil liberties protections consistent with section 248(a); and

“ (C) notice to potentially affected third parties as may be applicable;

“ (2) specify the reasons for the required action and the duration of such directive;

“ (3) minimize the impact of directives under this section by adopting the least intrusive means possible to secure the federal system or systems under the particular circumstances for the shortest time practicable; and

“ (4) notify the Director of the Office of Management and Budget and head of any affected agency immediately upon the issuance of directives under this section.

“ (b) When the Secretary determines that there is an imminent threat to federal systems and a directive under subsection (a) is not reasonably likely to result in a timely response to the threat, the Secretary may authorize use of protective capabilities under the Secretary’s control on communications or other system traffic transiting to or from or stored on a federal system without prior consultation with the affected agency for the purpose of ensuring the security of that system or other federal systems, provided that—

“ (1) the authorities under this subsection are not delegated below the level of Assistant Secretary;

“ (2) the Secretary or the Secretary’s designee immediately notifies the Director of the Office of Management and Budget, head of the affected agencies, and associated Chief Information Officers of any action taken under this subsection as to the reasons, duration, and nature of the action; and

“ (3) the Secretary’s actions are otherwise consistent with applicable law.

Legislative Language

CYBERSECURITY REGULATORY FRAMEWORK FOR COVERED CRITICAL INFRASTRUCTURE ACT

Sec. 1. Short Title.

This Title may be cited as the "Cybersecurity Regulatory Framework for Covered Critical Infrastructure Act."

Sec. 2. Purpose.

The purpose of this Title is to:

(1) enhance the cybersecurity of infrastructures determined by the Secretary to be critical to national security, national economic security, and national public health and safety;

(2) provide for consultation on matters pertaining to cybersecurity among sector-specific agencies with responsibility for critical infrastructure, agencies with responsibilities for regulating critical infrastructure, and agencies with expertise regarding services provided by critical infrastructure;

(3) facilitate public sector and private industry consultation and development of best cybersecurity practices by encouraging a national dialogue on cybersecurity vulnerabilities affecting critical infrastructure;

(4) establish workable frameworks for implementing cybersecurity minimum standards and practices designed to complement, not supplant, the scope or operation of currently-available security measures;

(5) to the maximum extent feasible and practicable, harmonize the designation of entities as covered critical infrastructure with existing infrastructure protection activities authorized pursuant to title II of the Homeland Security Act of 2002 (6 U.S.C. 121 et seq.);

(6) preserve principles of open government and support the free flow of information while protecting security and vulnerability-related information; and

(7) maintain a cyber environment that encourages efficiency and cost-effectiveness, innovation, and economic prosperity while also promoting safety, security, civil liberties, and privacy rights.

Sec.3. Designation of Covered Critical Infrastructure.

(a) Authority.—Pursuant to section 9 of this Title, the Secretary shall establish a process for designating entities as covered critical infrastructure.

(b) Requirements.—

(1) In general.—An entity may not be designated as covered critical infrastructure under subsection (a) unless:

(A) the incapacity or the disruption of the reliable operation of the entity, a system or asset it operates, or a service it provides would have a debilitating impact on national security, national economic security, national public health or safety; and

(B) the entity, a system or asset it operates, or a service it provides is dependent upon information infrastructure to operate, or is a part of information infrastructure and critical to its operation.

(2) Factors to be considered.—In designating entities under this section, the Secretary shall consider, but not be limited to, the following factors in order to evaluate the cybersecurity risks and consequences by sector, including:

(A) interdependencies among components of covered critical infrastructure (as designated under this section);

(B) the relative size of the entity in question; and

(C) the potential for the incapacity or disruption of the entity, a system or asset it operates, or a service it provides to cause severe, negative consequences to national security, national economic security, and national public health and safety.

(c) Establishment of Risk-Based Tiers.—In establishing a process for designating covered critical infrastructure, the Secretary shall establish risk-based tiers, and shall assign entities into the appropriate tier, based on the severity of, with regard to the entity, a system or asset it operates, or a service it provides:

(1) the threat of a cyber attack;

(2) its vulnerability to a cyber attack;

(3) the extent of consequences as a result of a cyber attack; and

(4) such other factors as the Secretary determines to be appropriate.|

(d) Lists of Covered Critical Infrastructure.—The Secretary shall establish lists of covered critical infrastructure and shall periodically review and update such lists. Inclusion on a list of covered critical infrastructure shall be considered a final action for purposes of judicial review in accordance with 5 U.S.C. 702.

Sec. 4. Risk Mitigation for Covered Critical Infrastructure.

(a) Cybersecurity Risks.—

(1) Pursuant to section 9 of this Title, the Secretary shall establish a process to:

(A) identify specific cybersecurity risks that must be mitigated to ensure the security of covered critical infrastructure; and

(B) review and designate frameworks to address such risks.

(2) The cybersecurity risks that must be mitigated may take into account the criticality of specific systems, assets, functions, or services and the impact of cybersecurity risks on such specific systems, assets, functions, or services; and may vary by sector and tier.

(3) The Secretary shall regularly update the identified cybersecurity risks.

(b) Frameworks for Addressing Cybersecurity Risks.—

(1) The Secretary shall request that representatives of organizations that coordinate or facilitate the development and use of voluntary consensus standards, representatives of appropriate voluntary consensus standards development organizations, appropriate representatives of State and local governments, agencies, and the private sector, including sector coordinating councils and information sharing and analysis centers, propose standardized frameworks for addressing cybersecurity risks.

(2) The Secretary shall, in consultation with appropriate private sector representatives, consider the extent to which the proposed frameworks enhance security in practice, including whether they:

(A) reasonably address identified cybersecurity risks;

(B) are cost-effective, including by prioritizing efforts toward critical systems, assets, functions, services, and actual risk, and minimizing the potential for burdens on or costs to efficiency, innovation, and economic prosperity;

(C) emphasize outcome-based metrics for measuring the practical effectiveness of mitigating identified cybersecurity risks and not solely compliance in implementation of measures or controls; and

(D) include practical evaluation focusing on performance, including testing for vulnerabilities and simulated threats and other tests that mimic real-time system performance under attack and stress.

(3) The Secretary, in consultation with the appropriate agencies, shall review the standardized frameworks proposed under paragraph (1), and as appropriate, using the criteria identified in paragraph (2), designate and periodically update the designation of one or more frameworks that satisfy those criteria, which may be tailored to address the unique nature of various sectors.

(4) If the Secretary determines that no standardized framework proposed under paragraph (1) meets the criteria in paragraph (2), the Secretary shall adopt a framework that meets the criteria set forth in paragraph (2). As part of such a process, the Secretary shall invite the Director of the National Institute of Standards and Technology to provide advice and guidance on any possible alternative framework or frameworks in consultation with appropriate public and private stakeholders.

(5) Frameworks shall not require the use of a particular measure, but shall leave the choice of particular measures to an entity to which the framework applies.

Sec. 5. Cybersecurity Plans.

The owners or operators of covered critical infrastructure shall develop cybersecurity plans that identify the measures selected by the covered critical infrastructure to address the cybersecurity risks in a manner that complies with the regulations promulgated, and are guided by an applicable framework designated, under section 4. The cybersecurity plans shall:

(1) be signed and attested by an accountable corporate officer of the owner or operator of the covered critical infrastructure;

(2) remain on file at the headquarters or primary operating location of the covered critical infrastructure; and

(3) be available for review, inspection, and evaluation by an evaluator pursuant to section 6, the Secretary, or a agency with responsibility for regulating the entity.

Sec. 6. Evaluations.

(a) In General.—Pursuant to section 9 of this Title, the Secretary shall establish a process to provide for, and develop requirements relating to:

(1) the selection of accreditors;

(2) the accreditation process for evaluators;

(3) the roles and responsibilities of evaluators in measuring the effectiveness of owners or operators of covered critical infrastructure in managing and mitigating cybersecurity risks; and

(4) generally-accepted evaluation practices.

(b) Accreditation and Evaluation Processes.—

(1) Agreement.—The Secretary shall enter into one or more agreements with a non-governmental entity or entities with expertise in managing or implementing accreditation and evaluation programs for consensus standards, or a similarly qualified private sector entity, to carry out accreditations and oversee the evaluation process established under this section.

(2) Selected Accreditor Process for Accrediting Evaluators.—To accredit evaluators under this section, an entity entering into an agreement with the Secretary under paragraph (1) (hereinafter referred to in this section as a "selected accreditor") shall conduct such activities as the Secretary determines to be necessary to effectively carry out accreditations of evaluators and oversee the evaluation process.

(3) Selected Accreditor Process for Monitoring Evaluators.—The Secretary and any selected accreditor may monitor and inspect the operations of any evaluator under this section to ensure that the evaluator is complying with the procedures and requirements established under subsection (a), and all other applicable requirements.

(4) Selected Accreditor Process for Revoking Accreditations of Evaluators.—If the Secretary or any selected accreditor determines that an evaluator is not meeting the procedures or requirements established under subsection (a), the selected accreditor shall:

(A) revoke the accreditation of the evaluator to conduct evaluations under this subsection; and

(B) review any evaluation conducted by the evaluator and report to the Secretary on the findings of the review, as necessary and appropriate.

(c) Roles and Responsibilities of Evaluators.—Covered critical infrastructure shall be evaluated by evaluators on a schedule determined by the Secretary. Such evaluations shall produce outcome-based metrics that measure the practical effectiveness of the measures selected by covered critical infrastructure under section 5 in mitigating the identified cybersecurity risks. Such evaluations shall be updated on no less than an annual basis.

Sec. 7. Disclosure.

(a) Annual Certifications.—Pursuant to section 9 of this Title, the Secretary shall require the Chief Executive Officer or other accountable corporate officer of the covered critical infrastructure to annually certify in filings made to the Securities and Exchange Commission or, in the case of privately-held covered critical infrastructure, to the Secretary:

(1) that the cybersecurity plan required by section 5 has been developed and is being implemented in an expeditious manner;

(2) that the evaluation required by section 6 has been completed according to the schedule set forth in such section; and

(3) whether the evaluation required by section 6 has concluded that the covered critical infrastructure is effectively mitigating identified cybersecurity risks.

(b) Public Disclosure of Cybersecurity Plans and Certifications.—Pursuant to section 9 of this Title, the Secretary shall require owners or operators of covered critical infrastructure to publicly disclose high-level summaries of the cybersecurity plans required by section 5 and the evaluations required by section 6 in a manner and form determined by the Secretary. Such disclosures shall not include proprietary information or other information indicating a critical weakness of the covered critical infrastructure.

(c) Notification of Cybersecurity Incidents.—

(1) In General.—Pursuant to section 9 of this Title, the Secretary shall require owners or operators of covered critical infrastructure to promptly report to the Secretary any significant cybersecurity incident.

(2) Notification to Appropriate Agencies.—The Secretary shall develop, with the approval of the Attorney General, internal reporting and dissemination procedures to notify appropriate agencies of any significant cybersecurity incident reported to the Secretary under paragraph (1).

(d) Protection from Public Disclosure.—Except as otherwise provided in this Title:

(1) security and vulnerability-related information developed or collected under this Title and provided to the Federal government, including aggregated analysis and data, shall be exempt from disclosure under section 552(b)(3) of title 5, United States Code; and

(2) pursuant to section 9 of this Title, security and vulnerability-related information developed or collected under this Title and provided to the Federal government, including aggregated analysis and data, shall be protected from public disclosure, except that this paragraph:

(A) does not prohibit the sharing of such information, as the Secretary determines to be appropriate in order to mitigate cybersecurity threats or further the official functions of a government agency; and

(B) does not authorize such information to be withheld from a committee of Congress authorized to request the information.

(e) Protection of Classified Information.—Nothing in this section permits the unauthorized disclosure of classified information.

Sec. 8. Enforcement.

(a) In General.—Pursuant to section 9 of this Title:

(1) the Secretary may conduct a review to determine if the covered critical infrastructure is sufficiently addressing the identified cybersecurity risks, including by reviewing the cybersecurity plan required by section 5 and the evaluation required by section 6, and by conducting periodic quality control evaluations. If the Secretary determines, after conducting such a review, that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks, the Secretary may:

(A) enter into discussions, or request another agency with sector-specific expertise to enter into discussions, with the owner or operator of the covered critical infrastructure on ways to improve the cybersecurity plan or the evaluation, which may include the provision of technical assistance;

(B) after discussions permitted in subparagraph (A), issue a public statement that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks; and

(C) take such other action as may be determined appropriate by the Secretary;

except that the Secretary shall not, in enforcing the provisions of this Title, issue a shutdown order, require use of a particular measure, or impose fines, civil penalties, or monetary liabilities on the owner or operator of the covered critical infrastructure as a result of such review; and

(2) the Secretary shall establish an administrative review process for covered critical infrastructure to appeal a finding under this subsection that the covered critical infrastructure is not sufficiently addressing the identified cybersecurity risks.

(b) Special Provisions for Federal Contracts.—The Secretary shall work with the Federal Acquisition Regulatory Council established under section 1302 of title 41, United States Code, to amend the Federal Acquisition Regulation, as may be necessary and appropriate, in conjunction with the implementation of provisions under this Title.

(c) Judicial Review.—Any action pursuant subsections (a)(1)(B) or (C) shall be considered a final action for purposes of judicial review in accordance with 5 U.S.C. 702.

Sec. 9. Rulemaking.

(a) In General.—The Secretary shall promulgate regulations pursuant to 5 U.S.C. 553 to carry out the provisions of this Title.

(b) Consultation.—Regulations promulgated under this section shall include:

(1) coordination with, and the obtaining of information from, the head of any:

(A) sector-specific agency with responsibility for critical infrastructure;

(B) agency with responsibilities for regulating the critical infrastructure; and

(C) agency with expertise regarding services provided by critical infrastructure; and

(2) consultation with, and the obtaining of information from, the private sector and appropriate representatives of State and local governments.

(c) Exemptions.—The Secretary, in consultation with the Director of the Office of Management and Budget, may exempt in appropriate part covered critical infrastructure from the requirements of this Title if the Secretary determines that a sector-specific regulatory agency has sufficient specific requirements in place to effectively mitigate identified cybersecurity risks.

Sec. 10. Definitions.

In this Title:

(1) Agency – The term "agency" has the meaning given that term in section 3502(1) of title 44, United States Code, as amended.

(2) Cybersecurity Threat.—The term "cybersecurity threat" means any action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information stored on or transiting an information system.

(3) Critical Infrastructure.—The term "critical infrastructure" has the meaning given that term in section 1016 of Public Law 107-56 (42 U.S.C. 5195c(e)).

(4) Incident.—The term "incident" has the meaning given that term in Chapter 35 of title 44, as amended.

(5) Secretary.—The term "Secretary" means the Secretary of Homeland Security.

(6) Sector-Specific Agency.—The term "sector-specific agency" shall have the meaning given that term in Homeland Security Presidential Directive-7, as issued by the President on December 17, 2003.

Legislative Language

SEC. 1. COORDINATION OF FEDERAL INFORMATION SECURITY POLICY.
(a) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by striking subchapters II and III and inserting the following:

‘‘SUBCHAPTER II—INFORMATION SECURITY

‘‘ **§ 3551. Purposes**

‘‘The purposes of this subchapter are to—

‘‘(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

‘‘(2) recognize the highly networked nature of the current Federal computing environment and provide effective government-wide management of policies, directives, standards, and guidelines, as well as effective and nimble oversight of and response to information security risks, including coordination of information security efforts throughout the Federal civilian, national security, and law enforcement communities;

‘‘(3) provide for development and maintenance of controls required to protect agency information and information systems and contribute to the overall improvement of agency information security posture; and

‘‘(4) provide a mechanism for improved security of agency information security programs and systems through a focus on continuous monitoring of agency information systems and streamlined reporting requirements rather than over prescriptive manual reporting.

‘‘ **§ 3552. Definitions**

‘‘ (a) Except as provided under subsection (b), the definitions under section 3502 of this title (including for “agency” and “information system”) shall apply to this subchapter.
‘‘ (b) In this subchapter:

‘‘ (1) The term ‘adequate security’ means security commensurate with the risk and magnitude of the harm resulting from the unauthorized access to or loss, misuse, destruction or modification of information.

‘‘ (2) The term ‘incident’ means an occurrence that—

‘‘ (A) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of an information system or the information that system controls, processes, stores, or transmits; or

“ (B) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.

‘‘ (3) The term ‘information security’ means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

‘‘ (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring proof of origin of data and authenticity;

‘‘ (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

‘‘ (C) availability, which means ensuring timely and reliable access to and use of information by authorized persons, processes, or devices.

‘‘ (4) The term ‘information technology’ has the meaning given that term in section 11101 of title 40.

‘‘ (5) The term ‘national security system’ means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—

‘‘ (A) the function, operation, or use of which—

‘‘ (i) involves intelligence activities;

‘‘ (ii) involves cryptologic activities related to national security;

‘‘ (iii) involves command and control of military forces;

‘‘ (iv) involves equipment that is an integral part of a weapon or weapons system; or

‘‘ (v) subject to subparagraph (C), is critical to the direct fulfillment of military or intelligence missions; or

‘‘ (B) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

‘‘ (C) Subparagraph (A)(v) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

‘‘ (6) The term “Secretary” means the Secretary of Homeland Security unless otherwise specified.

‘‘**§ 3553. Federal information security authority and coordination.—**

‘‘ (a) IN GENERAL—The Secretary of Homeland Security shall exercise primary responsibility within the executive branch for information security, including implementation of information security policies and directives and compliance with the requirements of this subchapter, except as provided in subsections (d) and (e).

‘‘ (b) The Secretary of Homeland Security shall—

“ (1) issue compulsory and binding policies and directives governing agency information security operations, and require implementation of such policies and directives, including—

‘‘ (A) policies and directives consistent with the standards promulgated under section 11331 of title 40 to identify and provide information security protections prioritized and commensurate with the risk and impact resulting from

the unauthorized access, use, disclosure, disruption, modification, or destruction of—

‘‘ (i) information collected or maintained by or on behalf of an agency; or

‘‘ (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

“ (B) minimum operational requirements for federal Government network operations centers and security operations centers to protect agency information systems and provide common situational awareness across all agency information systems;

‘‘ (C) reporting requirements, consistent with relevant law, regarding information security incidents;

‘‘ (D) requirements for agency-wide information security programs;

‘‘ (E) performance requirements and metrics for the security of agency information systems;

‘‘ (F) training requirements to ensure that agencies are able to fully and timely comply with direction issued by the Secretary under this subchapter;

‘‘ (G) training requirements regarding privacy, civil rights and civil liberties, and information oversight for agency information security personnel;

‘‘ (H) requirements for the annual reports to the Secretary under section 3554(c); and,

“ (I) any other information security operations or information security requirements as determined by the Secretary in coordination with relevant agency heads.

‘‘ (2) review agency information security programs required under section 3554(b);

“ (3) designate an entity to receive reports and information about information security incidents, threats, and vulnerabilities affecting agency information systems.

‘‘ (c) When issuing policies and directives under paragraph (b), the Secretary of Homeland Security shall consider any applicable standards or guidelines developed by the National Institute of Standards and Technology (NIST) and issued by the Secretary of Commerce under 40 U.S.C. 11331. The Secretary shall consult with the Director of the NIST when such policies and directives implement standards or guidelines developed by NIST.

‘‘ (d) The authorities of the Secretary of Homeland Security under this section shall not apply to national security systems. Information security policies, directives, standards and guidelines for national security systems shall be overseen as directed by the President and, in accordance with that direction, carried out under the authority of the heads of agencies that operate or exercise authority over such national security systems.

‘‘ (e) The authorities and responsibilities of the Secretary under paragraphs (1) and (2) of subsection (b) shall be carried out by the Secretary of Defense for non-national security systems under the control of the Department of Defense.

“ (f) Nothing in this subchapter shall be construed to alter or amend any law regarding the authority of any Head of a federal agency over such agency.

‘‘**§ 3554. Agency responsibilities**

‘‘ (a) The head of each agency shall—

‘‘ (1) be responsible for—

“ (A) complying with the policies and directives issued under section 3553.

‘‘ (B) providing information security protections commensurate with the risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of—

‘‘ (i) information collected or maintained by the agency or by a contractor of an agency or other organization on behalf of an agency; and

‘‘ (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

‘‘ (C) complying with the requirements of this subchapter, including—

‘‘ (i) information security standards promulgated under section 11331 of title 40;

“ (ii) information security policies, directives, standards and guidelines for national security systems issued as directed by the President; and

“ (iii) information security policies and directives for non-national security systems issued under section 3553(b).

‘‘ (D) ensuring that information security management processes are integrated with agency strategic and operational planning processes;

“ (E) reporting and sharing, for those agencies operating or exercising control of a national security system, information about information security incidents, threats, and vulnerabilities to the entity designated by the Secretary under section 3553(b)(3) and to other appropriate entities consistent with policies and directives for national security systems issued as directed by the President; and

‘‘ (F) reporting and sharing, for those agencies operating or exercising control of non-national security systems, information about information security incidents, threats, and vulnerabilities to the entity designated by the Secretary of Homeland Security under section 3553(b)(3) and to other appropriate entities to the extent consistent with policies and directives for non-national security systems as prescribed under section 3553(b).

‘‘ (2) ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through—

‘‘ (A) assessing the risk and impact that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

‘‘ (B) determining the levels of information security appropriate to protect such information and information systems in accordance with policies and directives issued under section 3553(b) of this title and standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

‘‘ (C) implementing policies, procedures, and capabilities to cost-effectively reduce risks to an acceptable level;

‘‘ (D) actively monitoring the effective implementation of information security controls and techniques; and

‘‘ (E) reporting information about information security incidents, threats, and vulnerabilities in a timely manner to the entity designated under section 3553(b)(3) in accordance with paragraph (1);

‘‘ (3) assess and maintain the resiliency of information technology systems critical to agency mission and operations;

‘‘ (4) designate the agency Inspector General (or, if the agency does not have an Inspector General, an independent entity selected in consultation with the Secretary) to conduct the annual independent evaluation required under section 3556; provided however, that the agency Inspector General may contract with an independent entity to perform such evaluation;

‘‘ (5) delegate the Chief Information Officer or equivalent (or to a senior agency official who reports to the Chief Information Officer or equivalent) the authority and primary responsibility to implement an agency-wide information security program, to be reviewed under section 3553(b)(2), and to provide information security for the information collected and maintained by the agency or by another agency, contractor, or other source on behalf of the agency and information systems that support the operations, assets, and mission of the agency, including those provided or managed by another agency, contractor, or other source, that includes—

‘‘ (A) overseeing the establishment and maintenance of an enterprise security operations capability that on a continuous basis can—

‘‘ (i) detect, report, respond to, contain, and mitigate information security incidents that impair adequate security of the agency’s information and information system, in a timely manner and in accordance with policies and directives issued under section 3553(b); and

‘‘ (ii) report any information security incident described under clause (i) to the entity designated under section 3553(b)(3) in accordance with applicable policies and directives;

‘‘ (B) developing, maintaining, and overseeing an agency-wide information security program as required in subsection (b);

‘‘ (C) developing, maintaining, and overseeing information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3553 and section 11331 of title 40;

‘‘ (D) training and overseeing agency personnel with significant responsibilities for information security with respect to such responsibilities; and

‘‘ (E) assisting the CIO or senior agency official concerning their responsibilities under paragraph (2);

‘‘ (6) delegate to appropriate agency officials who are responsible for particular agency systems or subsystems the responsibility to ensure and enforce compliance with all requirements of the agency’s information security program as outlined in paragraph (5) above in coordination with the senior agency official designated under that paragraph;

‘‘ (7) ensure that the agency has trained and cleared personnel sufficient to assist the agency in complying with the requirements of this subchapter and policies and directives issued under section 3553(b);

‘‘ (8) ensure that the Chief Information Officer or senior agency official designated under paragraph (5), in coordination with other senior agency officials, reports to the agency head on the effectiveness of the agency information security program, including the progress of remedial actions; and

‘‘ (9) ensure that the senior agency official designated under paragraph (5) possesses the necessary qualifications to administer the functions described in this subchapter and has information security duties as a primary duty of that official.

‘‘ (b) The agency-wide information security programs described in paragraph (a)(5) shall include—

‘‘ (1) the development and maintenance of a risk management strategy for information security that considers information security threats, vulnerabilities and consequences that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency including those provided or managed by another agency, contractor, or other source, that includes;

‘‘ (2) security testing commensurate with risk and impact;

‘‘ (3) mitigation of information security vulnerabilities commensurate with risk and impact;

‘‘ (4) policies and procedures that—

‘‘ (A) are based on the risk management strategy required by paragraph (1);

‘‘ (B) cost-effectively reduce information security risks to an acceptable level;

‘‘ (C) ensure that cost effective and adequate information security is addressed throughout the life cycle of each agency information system; and

‘‘ (D) ensure compliance with—

‘‘ (i) the requirements of this subchapter;

‘‘ (ii) information security policies and directives issued under section 3553(b); and

‘‘ (iii) any other applicable requirements;

‘‘ (5) information security, privacy, civil rights, civil liberties, and information oversight training that meets requirements issued in accordance with section 3553(b) to inform information security personnel with access to agency information systems, including contractors and other users of information systems that support the operations and assets of the agency, of—

‘‘ (A) information security risks associated with their activities; and

‘‘ (B) individual responsibilities in complying with agency policies and procedures designed to reduce those risks;

‘‘ (6) risk-based continuous monitoring of the operational status and security of agency information systems to enable evaluation of the effectiveness of and compliance with information security policies, procedures, and practices, including a relevant and appropriate selection of management, operational, and technical controls of information systems identified in the inventory required under section 3505(c);

‘‘ (7) a process for ensuring that remedial actions have been taken to address any deficiencies in the information security policies, procedures, and practices of the agency;

‘‘ (8) operation of appropriate technical capabilities in order to detect, mitigate, report, and respond to information security incidents, consistent with policies and directives issued under section 3553(b), including—

‘‘ (A) mitigating risks associated with such information security incidents;

‘‘ (B) notifying and consulting with the entity designated under section 3553(b)(3); and

‘‘ (C) notifying and consulting with, as appropriate—

‘‘ (i) law enforcement agencies and relevant Offices of Inspectors General;

‘‘ (ii) any other entity, in accordance with law and as directed by the President; and

‘‘(9) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

‘‘ (c) Each agency shall annually submit a report on its information security program and information systems to the Secretary in accordance with applicable policies and directives issued pursuant to section 3553(b).

‘‘ **§ 3555. Periodic assessments**

‘‘ (a) Except as provided in paragraph (b) the Secretary shall prepare, based on the annual agency reports required under section 3554(c), annual independent evaluations under section 3556, the results of any continuous monitoring, and other available information, periodic summaries of agency security programs and practices. Such summaries may—

‘‘ (1) assess the effectiveness of agency information security policies, procedures, and practices;

‘‘ (2) provide an overall assessment of federal government-wide agency information system security posture; and

‘‘ (3) include recommendations for improving agency specific and federal government-wide agency information system security;

‘‘ (b)(1) Periodic summaries described in (a) relating to national security systems shall be prepared as directed by the President.

‘‘ (2) Periodic summaries described in (a) relating to agency information systems under the control of the Department of Defense shall be prepared by the Secretary of Defense in accordance with government wide reporting requirements.

‘‘ (c) In conducting assessments under this section, the Secretary shall take appropriate actions to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and policies.

‘‘ (d) The Secretary of Homeland Security, in coordination with the Secretary of Defense, shall evaluate and report to Congress annually on the adequacy and effectiveness of the information security programs and practices summarized under this section.

‘‘ § 3556. Independent Evaluations

‘‘ (a) The Council of Inspectors General on Integrity and Efficiency, in consultation with the Director of Office of Management and Budget and Secretary, shall issue and maintain criteria for timely, cost-effective, risk-based, and independent evaluations of agency information security programs and practices in order to determine the effectiveness of such information security programs and practices. Such criteria shall include measures to assess whether agency information security programs include appropriate safeguards against disclosure of information where such disclosure may adversely affect information security.

‘‘ (b) Agencies shall perform an annual independent evaluation of agency information security programs and practices in accordance with the criteria developed under paragraph (a) to determine the effectiveness of such programs and practices.

‘‘ (c) Reports prepared under this section shall be provided to the Secretary upon delivery of the report by the agency head.

‘‘ (d) Evaluations involving national security systems shall be conducted as directed by President.”

‘‘ § 3557. Savings Provisions and Technical and Conforming Amendments

(a) SAVINGS PROVISIONS.—

(1) Policy and compliance guidance issued by the Director of the Office of Management and Budget prior to the effective date of this Act pursuant to section 3543(a)(1) of title 44 (as in effect prior to the effective date) shall continue in effect, according to its terms, until modified, terminated, superseded, or repealed pursuant to section 3553(b)(1) of title 44, as added by this Act.

(2) Standards and guidelines issued by the Secretary of Commerce or by the Director of the Office of Management and Budget prior to the effective date of this Act pursuant to section 11331(a)(1) of title 40 (as in effect prior to the effective date) shall continue in effect, according to their terms, until modified, terminated, superseded, or repealed pursuant to section 11331(a)(1), as added by this Act.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—

(1) TABLE OF SECTIONS.—The table of sections for chapter 35 of title 44 is amended by striking the matter relating to subchapters II and III and inserting the following:

‘‘SUBCHAPTER II—INFORMATION SECURITY

‘‘3551. Purposes.

‘‘3552. Definitions.

‘‘3553. Federal information security authority and coordination.

‘‘3554. Agency responsibilities.

‘‘3555. Periodic assessments.

“ 3556. Independent Evaluations.

“3557. Savings Provisions and Technical and Conforming Amendments.

(2) OTHER REFERENCES.—

(A) Section 1001(c)(1)(A) of the Homeland Security Act of 2002 (6 U.S.C. 511(c)(1)(A)) is amended by striking ‘‘section 3532(3)’’ and inserting ‘‘section 3551(b)’’.

(B) Section 2222(j)(6) of title 10 is amended by striking ‘‘section 3542(b)(2))’’ and inserting ‘‘section 3551(b)’’.

(C) Section 2223(c)(3) of title 10 is amended, by striking ‘‘section 3542(b)(2))’’ and inserting ‘‘section 3551(b)’’.

(D) Section 2315 of title 10 is amended by striking ‘‘section 3542(b)(2))’’ and inserting ‘‘section 3551(b)’’.

(E) Section 20(a)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3) is amended by striking ‘‘section 3532(b)(2)’’ and inserting ‘‘section 3551(b)’’.

(F) Section 8(d)(1) of the Cyber Security Research and Development Act (15 U.S.C. 7406(d)(1)) is amended by striking ‘‘section 3534(b)’’ and inserting ‘‘section 3554(b)’’.

SEC. 2. MANAGEMENT OF INFORMATION TECHNOLOGY. —

(a) IN GENERAL.— Section 11331 of title 40, United States Code, is amended by striking the section and inserting the following:

‘‘ **§ 11331 Responsibilities for federal information systems standards.**

‘‘ (a) Standards and Guidelines.—

‘‘ (1) Authority to prescribe.—Except as provided under paragraph (2), the Secretary of Commerce shall, in consultation with the Secretary of Homeland Security, on the basis of standards and guidelines developed by the National Institute of Standards and Technology pursuant to paragraphs (2) and (3) of section 20(a) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(a)), prescribe standards and guidelines pertaining to Federal information systems.

‘‘ (2) National security systems. —Standards and guidelines for national security systems shall be developed, prescribed, enforced, and overseen as directed by the President.

‘‘ (b) Mandatory Requirements.—

‘‘ (1) Authority to make mandatory.—The Secretary of Commerce shall make standards prescribed under subsection (a)(1) compulsory and binding to the extent determined necessary by the Secretary of Commerce to improve the efficiency of operation or security of Federal information systems.

‘‘ (2) Required mandatory standards.—

‘‘ (A) Standards prescribed under subsection (a)(1) shall include information security standards that—

‘‘ (i) provide minimum information security requirements as determined under section 20(b) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3(b)); and

‘‘ (ii) are otherwise necessary to improve the security of Federal information and information systems.`

‘‘ (B) Information security standards described in subparagraph (A) shall be compulsory and binding.

‘‘ (c) Authority to Disapprove or Modify. —The President may disapprove or modify the standards and guidelines referred to in subsection (a)(1) if the President determines such action to be in the public interest. The President's authority to disapprove or modify such standards and guidelines may be delegated to the Director of the Office of Management and Budget. Notice of such disapproval or modification shall be published promptly in the Federal Register. Upon receiving notice of such disapproval or modification, the Secretary of Commerce shall immediately rescind or modify such standards or guidelines as directed by the President or the Director of the Office of Management and Budget.

‘‘ (d) Exercise of Authority.—To ensure fiscal and policy consistency, the Secretary of Commerce shall exercise the authority conferred by this section subject to direction by the President and in coordination with the Director of the Office of Management and Budget.

‘‘ (e) Application of More Stringent Standards. —The head of an executive agency may employ standards for the cost-effective information security for information systems within or under the supervision of that agency that are more stringent than the standards the Secretary of Commerce prescribes under this section if the more stringent standards—

‘‘ (1) contain at least the applicable standards made compulsory and binding by the Secretary of Commerce; and

‘‘ (2) are otherwise consistent with directives and implementation memoranda issued under section 3553(b) of title 44.

‘‘ (f) Decisions on Promulgation of Standards. —The decision by the Secretary of Commerce regarding the promulgation of any standard under this section shall occur not later than 6 months after the submission of the proposed standard to the Secretary of Commerce by the National Institute of Standards and Technology, as provided under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

‘‘ (g) Definitions. —In this section:

‘‘ (1) Federal information system. —The term “Federal information system” means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

‘‘ (2) Information security. —The term “information security” has the meaning given that term in section 3552 of title 44.

‘‘ (3) National security system. —The term “national security system” has the meaning given that term in section 3552 of title 44.

(b) TECHNICAL AND CONFORMING AMENDMENTS.—Section 21of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4) is amended as follows:

(1) Section 21(b)(2) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4) is amended after ‘‘the Institute’’ by inserting ‘‘Secretary of Homeland Security’’.

(2) Section 21(b)(3) of the National Institute of Standards and Technology Act (15 U.S.C. 278g–4) is amended after ‘‘the Secretary of Commerce’’ by inserting ‘‘Secretary of Homeland Security’’.

Legislative Language

PERSONNEL AUTHORITIES RELATED TO CYBERSECUIRTY POSITIONS

Part 1: Recruitment and Retention of Cybersecurity Employees at the Department of Homeland Security

SECTION 1. RECRUITMENT AND RETENTION OF CYBERSECURITY AND COMMUNICATIONS EMPLOYEES

(a) DEFINITIONS.—In this section:

(1) DEPARTMENT.—The term ‘‘Department’’ means the Department of Homeland Security.

(2) SECRETARY.—The term ‘‘Secretary’’ means the Secretary of Homeland Security.

(3) QUALIFIED EMPLOYEE.—The term “qualified employee” means an employee who performs functions relating to the security of federal systems and critical information infrastructure.

(4) COLLECTIVE BARGAINING AGREEMENT.—The term “collective bargaining agreement” has the meaning given such term in section 7103(a)(8) of title 5.

(b) GENERAL AUTHORITY.—

(1) Appoint Personnel and Fix Rates of Pay. The Secretary may exercise, with respect to qualified employees of the Department, any authority of the Secretary of Defense with respect to civilian intelligence personnel under sections 1601, 1602, and 1603(a) of title 10, to the same extent, and subject to the same conditions and limitations, that the Secretary of Defense may exercise such authority with respect to civilian intelligence personnel of the Department of Defense.

(2) Scholarship Program. The Secretary may exercise, with respect to qualified employees of the Department, the authority of the Secretary of Defense with respect to civilian personnel under section 2200a of title 10, to the same extent, and subject to the same conditions and limitations, that the Secretary of Defense may exercise such authority with respect to civilian personnel of the Department of Defense.

(3) Plan for Execution of Authorities.—Not later than 120 days of enactment of this Act, the Secretary shall submit a report to the appropriate Committees of Congress with a plan for the execution of the authorities under this subchapter.

(4) Collective Bargaining Agreements. Nothing in section (b)(1) may be construed to impair the continued effectiveness of a collective bargaining agreement with respect to an Office, Component, Subcomponent, or equivalent of the Department that is a successor to

an Office, Component, Subcomponent, or equivalent of the Department covered by the agreement before the succession.

(5) The Secretary, in coordination with the Director, Office of Personnel Management, shall prescribe regulations for the administration of this subchapter.

(c) MERIT SYSTEM PRINCIPLES AND CIVIL SERVICE PROTECTIONS: APPLICABILITY

(1) Applicability of Merit System Principles.—Section 2301 of title 5 shall apply to the exercise of authority under this subchapter.

(2) Civil Service Protections.—The Secretary shall apply the civil service protections established in section 1612(b) of title 10 with respect to the exercise of authority under section 1601 of title 10.

(d) ANNUAL REPORT.—Not later than 1 year after the date of enactment of this Act, and every year thereafter for 4 years, the Secretary shall submit to the appropriate committees of Congress a detailed report that—

(1) discusses how the actions taken during the period of the report are fulfilling the Department's critical need to recruit and retain qualified employees;

(2) provides metrics on the following actions occurring during the reporting period, including—

(i) the number of qualified employees hired by occupation and grade/level or pay band;

(ii) the total number of veterans hired;

(iii) the number of separations of qualified employees;

(iv) the number of retirements of qualified employees; and

(v) the number and amounts of recruitment, relocation, and retention incentives paid to qualified employees by occupation and grade/level or pay band.

Part 2: Reactivation and Streamlining of Government-wide Information Technology Exchange Program.

(a) Reactivation of Program.—Section 3702(d) of title 5, United States Code, is amended by striking ", except that" and all that follows through "this chapter".

(b) Eligible Employees.—Section 3702(a) of such title is amended—

(1) in the matter preceding paragraph (1), by striking “An eligible employee is an individual who—” and inserting “An employee shall be eligible for such an assignment only if the employee—”;

(2) in paragraph (2), by striking “an exceptional performer by the individual’s current employer” and inserting “by the employee’s current employer to be a highly skilled and valued employee who excels in the performance of the employee’s duties and who would excel in the assignment”;

(3) in the third sentence—

(A) by striking “An employee of an agency shall be eligible to participate in this program” and inserting “In addition, an employee shall be eligible for such an assignment”;

(B) by striking “employed at the” and all that follows through “excepted service,” and inserting “compensated at not less than the GS-11 level (or the equivalent)”; and

(C) by inserting “(44 U.S.C. 3501 note)” after “of 2002”.

(c) Agreements.—Section 3702(b) of such title is amended—

(1) in the first sentence, by striking “between the agency and” and inserting “among the agency, the private sector organization, and”;

(2) in the second sentence, by inserting “paid by the agency, exclusive of salary” before the period at the end of paragraph (2); and

(3) in the third sentence, by inserting “for which an employee is liable” after “An amount”.

(d) Assignments.—Section 3702(c) of such title is amended by striking “Assignments” and inserting “An assignment under this section”.

(e) Small Business Concerns.—Section 3703(e) of such title is amended—

(1) in paragraph (1), by inserting “that the agency has a goal” after “to ensure”; and

(2) in paragraph (3)—

(A) by striking “comply with” in the first sentence and inserting “meet the goal specified in”; and

(B) by striking “noncompliance with” in subparagraph (C) and inserting “not meeting the goal specified in”.

(f) Revision of Covered Employment Fields.—Section 3702 of such title is amended by striking “management” in subsections (a)(1), (a)(3), and (f)(2).

(g) Regulations.—Regulations required to implement the amendments to chapter 37 of title 5, United States Code, made by this section shall be prescribed not later than 365 days after the date of the enactment of this Act.

Legislative Language

PREVENTING RESTRICTIONS ON DATA CENTER LOCATIONS

(a) Prohibition. Except where expressly authorized by federal law, no law, rule, regulation, or order, or other administrative action of any State or any political subdivision thereof shall require that a business entity locate a data center in such State or political subdivision thereof as condition precedent to the certification, licensure, or any other approval relating to the operation of such business entity.

(b) Definitions. For the purposes of this section -

1. The term "data center" means any facility that primarily contains electronic equipment used to process, store, and transmit digital information and that processes, stores, or transmits digital information in or affecting interstate or foreign commerce.

2. The term "business entity" means any person, group of persons, or organization performing or engaging in any activity, enterprise, profession, or occupation for gain, benefit, advantage, or livelihood, whether for profit or not for profit, but does not mean any State or political subdivision thereof.